SonicWALL Network Anti-Virus

SONICWALL

Contents

Copyright Notice

Specifications and descriptions subject to change without notice.

Limited Warranty

SonicWALL, Inc. warrants that SonicWALL Network Anti-Virus will perform in accordance to the accompanying written materials for a period of ninety (90) days from the date of receipt.

SonicWALL Inc.'s and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the PRODUCT has resulted from accident, abuse, or misapplication. Any replacement PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

In no event shall SonicWALL or its suppliers be liable for any damages whatsoever (including, without limitation, special, incidental, indirect, or consequential damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the PRODUCT.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL's liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state.

By using this Product, you agree to these limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

No dealer, agent, or employee of SonicWALL is authorized to make any extension or addition to this warranty.

Introduction

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses don't have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as "ILOVEYOU" and Melissa, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Network Anti-Virus prevents occurrences like these and offers a new approach to virus protection. The SonicWALL family of firewalls constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWALL restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

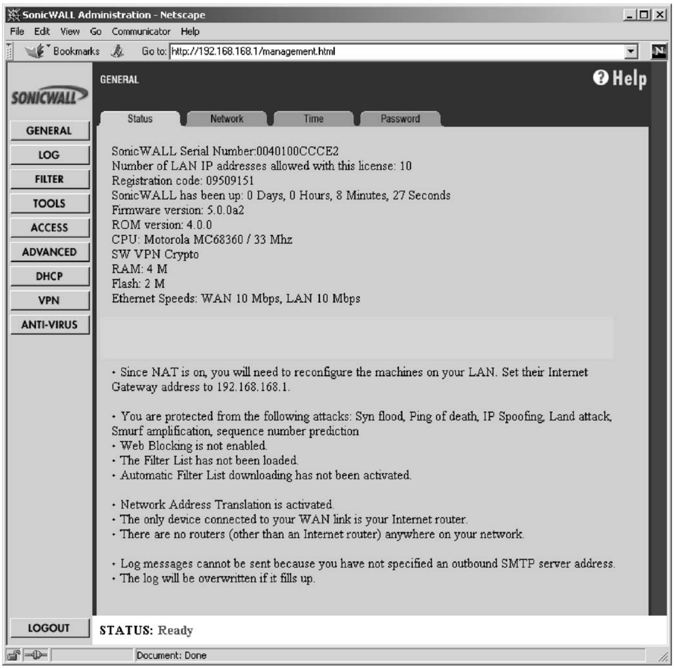
Managing Network Anti-Virus

This section contains detailed information on the activation, installation and configuration of the SonicWALL Network Anti-Virus subscription. Network Anti-Virus is configured from the SonicWALL Management Interface.

This section describes:

- **Activating the Network Anti-Virus Subscription**
- **Configuring Network Anti-Virus**
- **Managing Network Anti-Virus Subscriptions and Reports**
- **Configuring the Network Anti-Virus E-mail Filter**

To access the Anti-Virus feature in the SonicWALL, click **General** on the left side of the browser window, and then click **Status** at the top of the window.



SonicWALL Serial Number:0040100CCCE2
Number of LAN IP addresses allowed with this license: 10
Registration code: 09509151
SonicWALL has been up: 0 Days, 0 Hours, 8 Minutes, 27 Seconds
Firmware version: 5.0.0a2
ROM version: 4.0.0
CPU: Motorola MC68360 / 33 Mhz
SW VPN Crypto
RAM: 4 M
Flash: 2 M
Ethernet Speeds: WAN 10 Mbps, LAN 10 Mbps

- Since NAT is on, you will need to reconfigure the machines on your LAN. Set their Internet Gateway address to 192.168.168.1.

- You are protected from the following attacks: Syn flood, Ping of death, IP Spoofing, Land attack, Smurf amplification, sequence number prediction
- Web Blocking is not enabled.
- The Filter List has not been loaded.
- Automatic Filter List downloading has not been activated.

- Network Address Translation is activated.
- The only device connected to your WAN link is your Internet router.
- There are no routers (other than an Internet router) anywhere on your network.

- Log messages cannot be sent because you have not specified an outbound SMTP server address.
- The log will be overwritten if it fills up.

STATUS: Ready

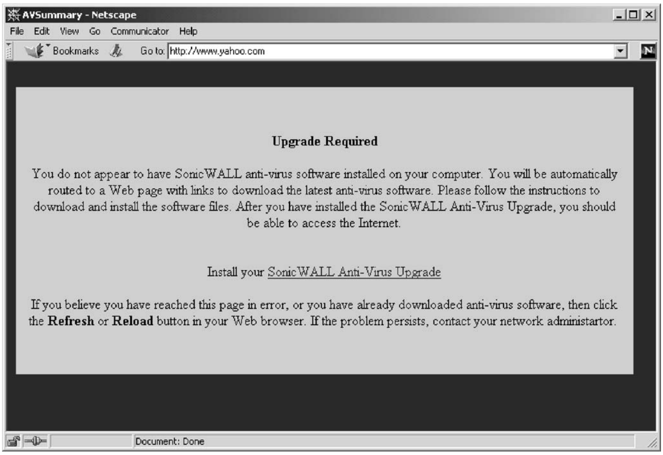
This window displays the current status of the SonicWALL. It contains an overview of the SonicWALL configuration as well as any other important messages. If a message stating, “This SonicWALL is not yet registered” is displayed, then it is necessary to complete the online registration before activating the Network Anti-Virus subscription. Click the link to <http://www.mysonicwall.com and complete the online registration process.

To activate SonicWALL Network Anti-Virus, the SonicWALL must have firmware version 5.0.0 or greater. See the SonicWALL Internet Security Appliance User Guide for instructions on updating to the latest SonicWALL firmware.

The optional Network Anti-Virus subscription must be registered to activate Anti-Virus enforcement. The **Activation Key** is displayed on the back of this manual.

Activating the Network Anti-Virus Subscription

1. Click **Anti-Virus** on the left side of the browser window.



AVSummary - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://www.yahoo.com
Document: Done

Upgrade Required

You do not appear to have SonicWALL anti-virus software installed on your computer. You will be automatically routed to a Web page with links to download the latest anti-virus software. Please follow the instructions to download and install the software files. After you have installed the SonicWALL Anti-Virus Upgrade, you should be able to access the Internet.

Install your SonicWALL Anti-Virus Upgrade

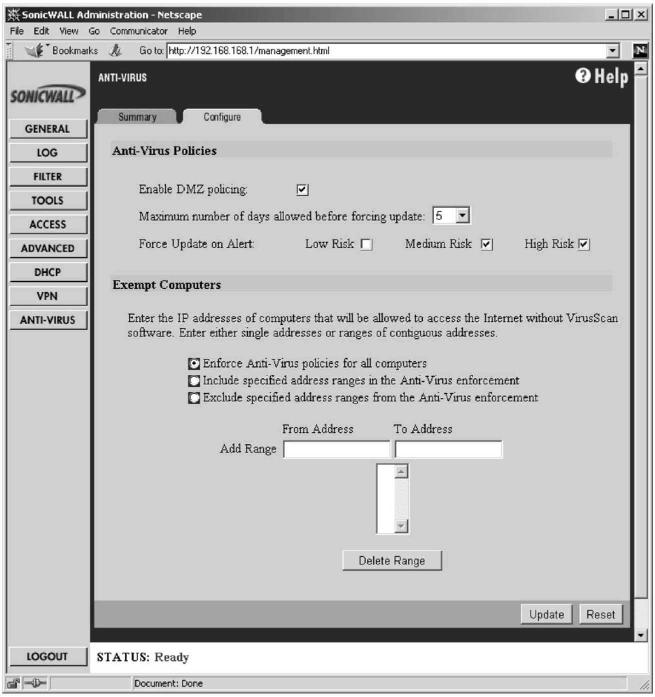
If you believe you have reached this page in error, or you have already downloaded anti-virus software, then click the **Refresh** or **Reload** button in your Web browser. If the problem persists, contact your network administartor.

2. Click the **Activate your Network Anti-Virus Subscription** link. Enter the **Activation Key** located on the back of this manual in the **Anti-Virus License Key** field. Then enter a password in the **Anti-Virus Password** and **Verify Password** fields. The Anti-Virus password is used to add or renew licenses or to view network reports. The password must be between 6 to 12 alphanumeric characters in length.

3. After entering the required information, click **Submit**. The operation takes several seconds to complete. Once the Network Anti-Virus activation is complete, a window appears confirming the activation and displaying the number of registered Network Anti-Virus Licenses.

Configuring Network Anti-Virus

After activating the subscription, enable and configure the Anti-Virus enforcement policy. Click **Anti-Virus** on the left side of the browser window and then click **Configure**.



Anti-Virus Policies

Enable DMZ policing: ☑

Maximum number of days allowed before forcing update: 5

Force Update on Alert: Low Risk □ Medium Risk ☑ High Risk ☑

Exempt Computers

Enter the IP addresses of computers that will be allowed to access the Internet without VirusScan software. Enter either single addresses or ranges of contiguous addresses.

● Enforce Anti-Virus policies for all computers
○ Include specified address ranges in the Anti-Virus enforcement
○ Exclude specified address ranges from the Anti-Virus enforcement

Add Range From Address ______ To Address ______

STATUS: Ready

The following options can be configured in the SonicWALL:

- **Enable DMZ policing**

  Selecting this option enforces the anti-virus policy on computers located on the DMZ. This option applies to SonicWALL DMZ, XPRS2, PRO, or PRO-VX. This feature is not available for the SonicWALL SOHO2 or TELE2.

- **Disable policing from LAN to DMZ**

  Choosing this option allows computers on the LAN to access computers on the DMZ, even if anti-virus software has not been installed on the LAN machines. This option applies only to SonicWALL DMZ, XPRS2, PRO, or PRO-VX.

- **Maximum number of days allowed before forcing update**

  Selecting this option defines the maximum number of days users may access the Internet before the SonicWALL requires the latest version of VirusScan ASaP to be downloaded.

- **Force Update on Alert**

  SonicWALL, Inc. broadcasts virus alerts to all SonicWALL appliances with an Anti-Virus subscription. Three levels of alerts available:

  Low Risk - A virus that has not been reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.

  Medium Risk - If a virus is found in the field, and if it uses a less common infection mechanism, it is assigned a medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly, it can be upgraded to a high risk if the virus is getting more and more widespread.

  High Risk - To be assigned a high-risk rating, it is necessary that a virus be reported often or very often in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk might be assigned even with a lower level of prevalence.

When an alert is received with this option enabled, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet*.* This option overrides the **Maximum number of days allowed before forcing update** selection.

In addition, every virus alert is logged, and an alert message is sent to the administrator. Please refer to the Logging and Alerts section of the SonicWALL Internet Security Appliance User Guide for instructions on configuring log and E-mail alerts.

SonicWALL Network Anti-Virus currently supports Windows 95, 98, NT and 2000 platforms. In order to access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement. There are three options for defining exempt computers:

- **Enforce Anti-Virus policies for all computers**

  Selecting this option forces computers to install VirusScan ASaP in order to access the Internet or the DMZ. This is the default configuration.

- **Include specified address range in the Anti-Virus enforcement**

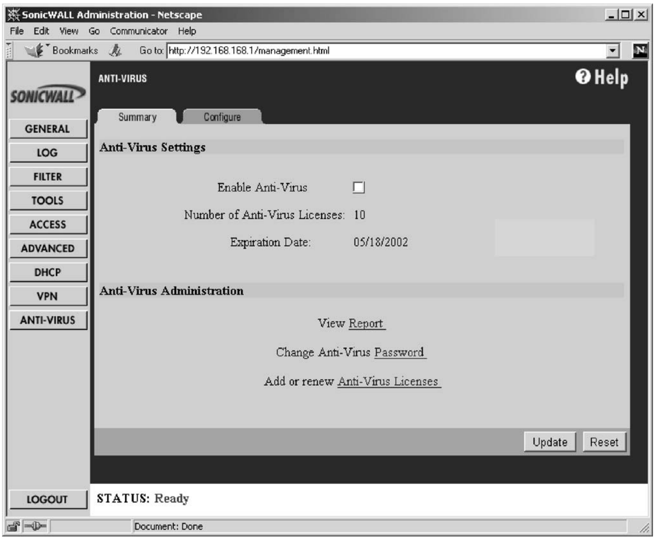
  Choosing this option allows the administrator to define a range of IP addresses to receive Anti-Virus enforcement. If you select this option, specify a range of IP addresses to be enforced. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses.

- **Exclude specified address range in the Anti-Virus enforcement**

  Selecting this option allows the administrator to define a range of IP addresses that are exempt from Anti-Virus enforcement. If you select this option, specify the range of IP addresses are exempt. Any computer requiring unrestricted Internet access needs a static IP address within the specified range of IP addresses.

The Network Anti-Virus Summary Tab

Click **Anti-Virus** on the left side of the browser window, and then click **Summary** at the top of the window.



Anti-Virus Settings

Enable Anti-Virus □

Number of Anti-Virus Licenses: 10

Expiration Date: 05/18/2002

Anti-Virus Administration

View Report

Change Anti-Virus Password

Add or renew Anti-Virus Licenses

STATUS: Ready

Anti-Virus Settings

The **Summary** tab displays the following information:

- **Enable Anti-Virus**

  After activating the Network Anti-Virus subscription, selecting the **Enable Anti-Virus** check box enables Anti-Virus enforcement on the network.

- **Number of Anti-Virus Licenses**

  The number of the current licenses that have been registered for the firewall.

***Note**: Each anti-virus license allows the use of SonicWALL Network Anti-Virus on one computer for a 12-month period.*

- **Expiration Date**

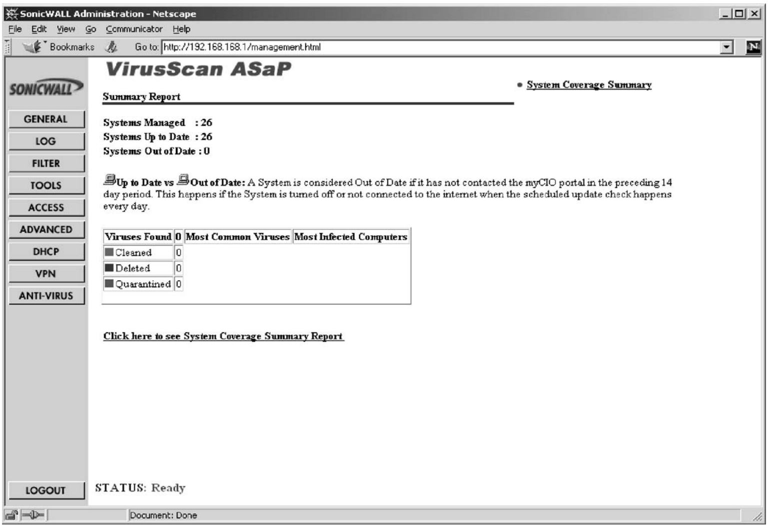
  The expiration date of the current subscription is displayed.

Anti-Virus Administration

The **Anti-Virus Administration** section provides links to reports summarizing Anti-Virus activity on the network. Administrative activities such as changing passwords and renewing or adding licenses are also accessed here.

Reports

To view Network Anti-Virus statistics and reports, click the link labeled **View Report**. The Authentication window appears. Enter the Anti-Virus password in the **Anti-Virus Password** field and click **Submit**.


SonicWALL Administration - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://192.168.168.1/management.html
SONICWALL
GENERAL
LOG
FILTER
TOOLS
ACCESS
ADVANCED
DHCP
VPN
ANTI-VIRUS
LOGOUT
Document: Done

VirusScan ASaP

• System Coverage Summary

Summary Report

Systems Managed : 26
Systems Up to Date : 26
Systems Out of Date : 0

Up to Date vs Out of Date: A System is considered Out of Date if it has not contacted the myCIO portal in the preceding 14 day period. This happens if the System is turned off or not connected to the internet when the scheduled update check happens every day.

Viruses Found	0	Most Common Viruses	Most Infected Computers
■ Cleaned	0		
■ Deleted	0		
■ Quarantined	0		

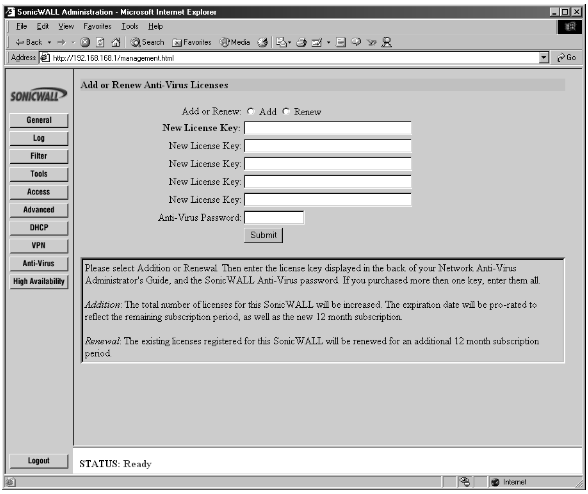
Click here to see System Coverage Summary Report

STATUS: Ready

This window displays general information about Network Anti-Virus. Information about the number of desktops protected, and the number of updated and outdated desktops is shown at the top right corner of the window. The table offers information about the viruses found, the most common viruses and the most infected computers on the network.

Add or Renew Licenses

To manage Anti-Virus licenses, click the link labeled **Add or Renew Anti-Virus Licenses** in the **Anti-Virus Summary** tab.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.1/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
Internet

Add or Renew Anti-Virus Licenses

Add or Renew: ○ Add ○ Renew

New License Key:

New License Key:

New License Key:

New License Key:

New License Key:

Anti-Virus Password:

Submit

Please select Addition or Renewal. Then enter the license key displayed in the back of your Network Anti-Virus Administrator's Guide, and the SonicWALL Anti-Virus password. If you purchased more then one key, enter them all.

Addition: The total number of licenses for this SonicWALL will be increased. The expiration date will be pro-rated to reflect the remaining subscription period, as well as the new 12 month subscription.

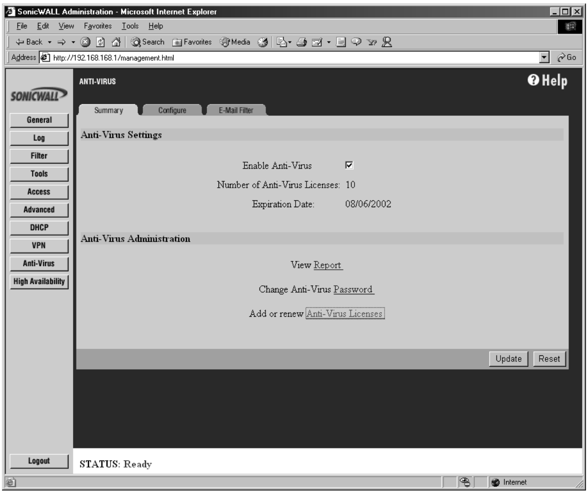
Renewal: The existing licenses registered for this SonicWALL will be renewed for an additional 12 month subscription period.

STATUS: Ready

Adding More Licenses

The standard SonicWALL Network Anti-Virus subscription package can be used to activate Network Anti-Virus, to increase the number or Anti-Virus licenses or to renew the current subscription. Since a Network Anti-Virus Activation Key may not be reused, additional subscription packages are required to add or renew Anti-Virus licenses.

1. Select the **Add** option at the top of the **Add or Renew Licenses** window.
2. Enter the Activation Key displayed on the back of the Network Anti-Virus Administrator's Guide in the **New License Key** field.
3. Create and enter an Anti-Virus password in the **Anti-Virus Password** field, and click **Submit**. The operation takes a few seconds to complete. Once completed, the new number of Anti-Virus licenses appears in the Anti-Virus **Summary** window.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.168.1/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
High Availability
Logout
ANTI-VIRUS
Help
Summary
Configure
E-Mail Filter
Update
Reset
Internet

Anti-Virus Settings

Enable Anti-Virus ☑

Number of Anti-Virus Licenses: 10

Expiration Date: 08/06/2002

Anti-Virus Administration

View Report

Change Anti-Virus Password

Add or renew Anti-Virus Licenses

STATUS: Ready

***Note**: When adding licenses, a new subscription is granted with a single new number of licenses and a single expiration date. Multiple grants are not tracked. The time remaining on the previous subscription is combined with the new 12-month period of the additional grant to create a single subscription.*

Renewing the Current Subscription

A **Subscription Renewal** is the process of renewing the existing Anti-Virus subscriptions and the number of Anti-Virus licenses does not increase. If the current subscription has 10 users, a 10-user renewal extends the subscription period by one year, but the total number of users remains the same.

***Note**: When renewing a Network Anti-Virus subscription, the number of licenses for subscription renewal must be equal to the number of licenses in the current subscription.*

To renew the current subscription, complete the following steps:

1. Select the **Renewal** option at the top of the Add or Renew Licenses window.

2. Enter the Activation Key displayed on the back of the Network Anti-Virus Administrator's Guide in the **New License Key** field.

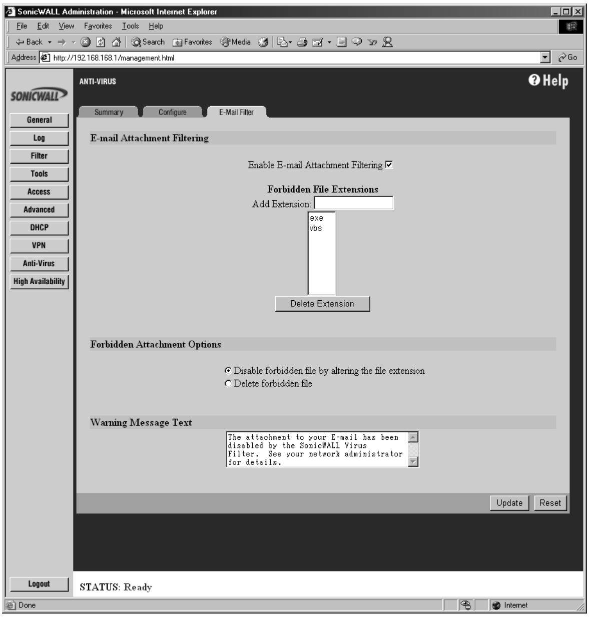
3. Enter the Anti-Virus password in the **Anti-Virus Password** field, and click **Submit**. The operation takes a few seconds to complete. Once completed, the new expiration date appears in the Anti-Virus **Summary** window.

Network Anti-Virus E-Mail Filter

The **Network Anti-Virus E-Mail Filter** allows the administrator to selectively delete or disable inbound E-mail attachments as they pass through the SonicWALL. This feature provides control over executable files and scripts, and applications sent as E-mail attachments.

***Note**: The Anti-Virus E-mail Filter is compatible only with SMTP protocol. It does not filter POP3 e-mail. Also, the SMTP mail server must be configured on the LAN side of the SonicWALL.*

Click **Anti-Virus** on the left side of the browser window, and then click the **E-Mail Filter** tab.



E-mail Attachment Filtering

Enable E-mail Attachment Filtering ☑

Forbidden File Extensions

Add Extension:

exe
vbs

Forbidden Attachment Options

● Disable forbidden file by altering the file extension
○ Delete forbidden file

Warning Message Text

```
The attachment to your E-mail has been
disabled by the SonicWALL Virus
Filter.  See your network administrator
for details.
```

STATUS: Ready

E-Mail Attachment Filtering

The **E-mail Attachment Filtering** section configures the file extensions that are filtered by the SonicWALL.

- **Enable E-Mail Attachment Filtering**

  Select this check box to filter E-mail attachments.

- **Forbidden File Extensions**

  Enter the file extensions to be filtered in the **Add Extension** field. Hackers commonly spread viruses through Visual Basic and Windows Executable files, therefore "vbs" and "exe" are provided as default extensions for this feature.

Forbidden Attachment Options

In this section, the administrator chooses the action that the SonicWALL performs when filtering E-mail attachments. The attached file can either be deleted or it can be disabled by altering the file extension. In either case, the original E-mail text is still sent to the intended recipient.

- **Disable forbidden file by altering the file extension**

  Select this option to disable forbidden attachment files as they pass through the SonicWALL. The SonicWALL replaces the third character of file extensions with "_". If the E-mail attachment is a valid file, the E-mail recipient may return the attachment to its original file extension without damaging the file.

- **Delete forbidden file**

  Select this option to delete forbidden attachment files as they pass through the SonicWALL.

Warning Message Text

This is a warning message that can be customized and added to E-mails filtered by the **Network Anti-Virus E-mail Filter**. Enter the desired warning message in the **Warning Message Text** box. Up to 256 alphanumeric characters may be entered.

When you have configured the **E-mail Filter** settings, click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

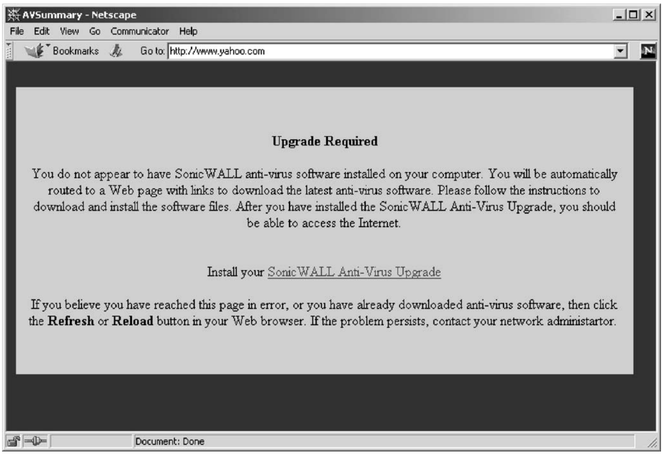
Installing the Network Anti-Virus Client

After installing, configuring and enabling the SonicWALL Network Anti-Virus Subscription, each computer designated for virus protection begins the automated installation of VirusScan ASaP. VirusScan ASaP is an Internet-based, managed anti-virus service. It is based on Network Associates' myCIO.com VirusScan ASaP technology and provides continuous protection of the entire desktop environment against viruses.

In most cases, VirusScan ASaP automatically removes other anti-virus products and their components.

Installing on Windows 95/98/NT/2000 computers

When the Network Anti-Virus is enabled, all computers on the network are automatically re-directed to the page shown below:


AVSummary - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://www.yahoo.com
Document: Done

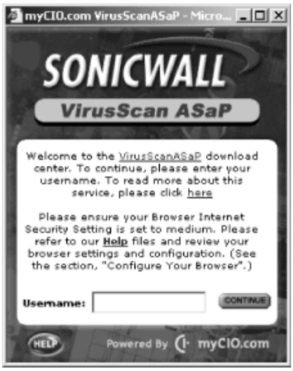
Upgrade Required

You do not appear to have SonicWALL anti-virus software installed on your computer. You will be automatically routed to a Web page with links to download the latest anti-virus software. Please follow the instructions to download and install the software files. After you have installed the SonicWALL Anti-Virus Upgrade, you should be able to access the Internet.

Install your SonicWALL Anti-Virus Upgrade

If you believe you have reached this page in error, or you have already downloaded anti-virus software, then click the **Refresh** or **Reload** button in your Web browser. If the problem persists, contact your network administartor.

The user clicks on the link to access the pages required for installation of the application. If Netscape is being used as the browser, the user is prompted to first install a plug-in that allows the VirusScan service to operate. After loading the plug-in, the following screen appears.



Welcome to the VirusScanASaP download center. To continue, please enter your username. To read more about this service, please click here

Please ensure your Browser Internet Security Setting is set to medium. Please refer to our **Help** files and review your browser settings and configuration. (See the section, "Configure Your Browser".)

Username:

Enter a unique username and click **Continue** to begin the VirusScan ASaP installation. After restarting the computer, Internet access is allowed.

For some configurations of **Windows NT** and **Windows 2000** workstations, the installation is slightly different, especially if the user does not have administrative or software installation privileges on the computer. Before the installation of VirusScan ASaP, an executable must be run on each workstation that allows VirusScan ASaP to be installed. This file can be downloaded from ftp://ftp.sonicwall.com/pub/software/ and is called myCIOAgtInstall.exe. This allows users without administrative rights to install VirusScan ASaP.

This file can be installed either locally or with various distribution products, such as Microsoft SMS, or Tivoli. The myCIOAgtInstall.exe file can be launched from a logon script, but it must be executed by a user with local administrator privileges. Once this application has been executed, the user can proceed with the installation. The following is a summary of the actions required to load VirusScan ASaP on an NT or 2000 workstation where the user does not have local access:

1. Download the executable file called MyCIOAgtInstall.Exe
2. Run MyCIOAgtInstall.exe on the workstation.
3. Proceed with normal installation

Alternatively, local administrator privileges can be granted to users, allowing full access to VirusScan ASaP downloads. Consult Microsoft documentation for the operating system in use for this procedure.

Proxy Support

Proxy authentication support is limited to anonymous and Windows NT challenge/response authentication. Basic authentication is not supported at this time. It is recommended that the HTTP proxy port be configured to port 80. Under some circumstances where Internet connection bandwidth is limited, the proxy server inactivity timeout should be configured for a longer period of time to avoid failed downloads.

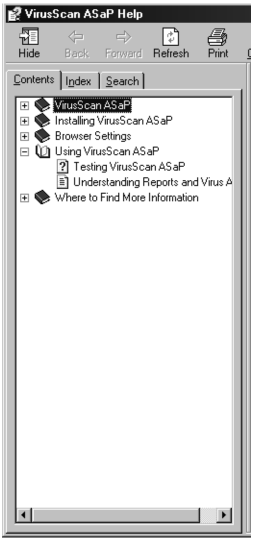
VirusScan ASaP Client User Information

After the **VirusScan ASaP** Client is installed, there are a few functionalities available to the user.

Testing VirusScan ASAP Client

To test the **VirusScan ASAP** client, you can download the EICAR Standard AntiVirus Test file which allows the client to detect a virus and display an alert. This file DOES NOT contain a virus, and cannot harm your system. To download the EICAR file, follow the steps below:

1. Press Control(CTL) and Shift, then with the cursor over the MyCIO icon , right mouse click.
2. A second menu appears that has more menu items than the standard menu. Click **Help** to view the **Online Help** menu.



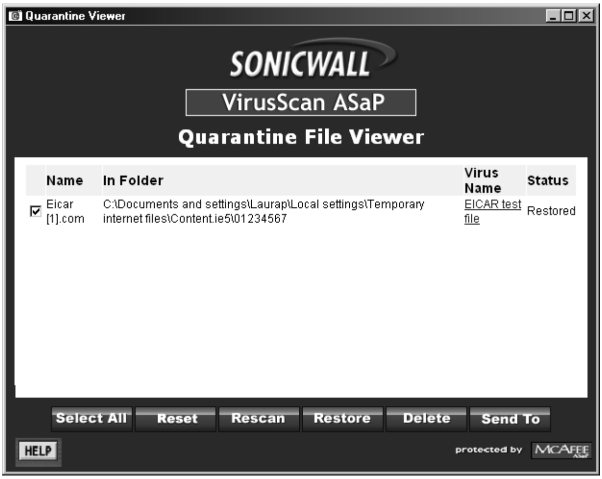
3. Select **Testing Virus Scan ASaP**, and follow the instructions on the help page.
4. If the client is installed properly, the VirusScan ASaP client interrupts the download, and displays a virus alert diaglog box.
5. If the client is installed incorrectly, the file is downloaded without interruption, and you should re-install the client software.

Advanced Menu for VirusScan ASaP Client

The Advanced Menu for **VirusScan ASaP** client is accessed by pressing the Control (Ctrl) button and the Shift button, then right clicking the MyCIO icon in the system tray at the bottom right of the screen. Not only can you select a directory, file, or hard drive for virus scanning, but you can also display the **Quarantine Viewer** and **Enable/Disable VShield**.

Quarantine Viewer

Quarantine Viewer displays any virus information about the **VirusScan ASaP** client, and where they were located before cleaning from your computer. You can **Delete** the information files, **Send** them to your system administrator, **Rescan** the infected files, or **Restore** the cleaned file to your system.



	Name	In Folder	Virus Name	Status
☑	Eicar [1].com	C:\Documents and settings\Laurap\Local settings\Temporary internet files\Content.ie5\01234567	EICAR test file	Restored

If the infected file cannot be cleaned by VirusScan, the infected file is deleted from your system, and a window displaying an alert dialogue box counts down the seconds until the window is closed.

Enable/Disable VScan

You can disable the **VScan** to install software as anti-virus software can interfere with some software installations. Be sure to enable the **VScan** after any software installation as you are now vulnerable to viruses.

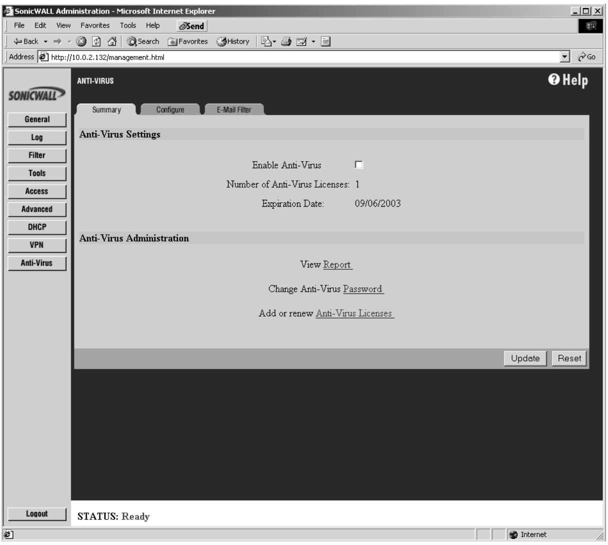
About VirusScan ASaP

Click the menu item, **About VirusScan ASaP**, to review the last time the client was updated, and the current virus engine used for scanning.

Anti-Virus License Sharing

Anti-Virus License Sharing allows you to distribute one or more Anti-Virus licenses among multiple firewalls. License sharing assigns a License Sharing Group (LSG) to a firewall from which this feature is activated. You may then add other firewalls to the LSG, by their serial numbers and assign them Anti-Virus licenses from the pool of remaining available licenses in the LSG. To set up a License Sharing Group, follow the directions below:

1. Log into the Management station and click **Anti-Virus**.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Send
Back Search Favorites History
Address http://10.0.2.132/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
Logout
ANTI-VIRUS
Help
Summary
Configure
E-Mail Filter
Update
Reset
Internet

Anti-Virus Settings

Enable Anti-Virus □

Number of Anti-Virus Licenses: 1

Expiration Date: 09/06/2003

Anti-Virus Administration

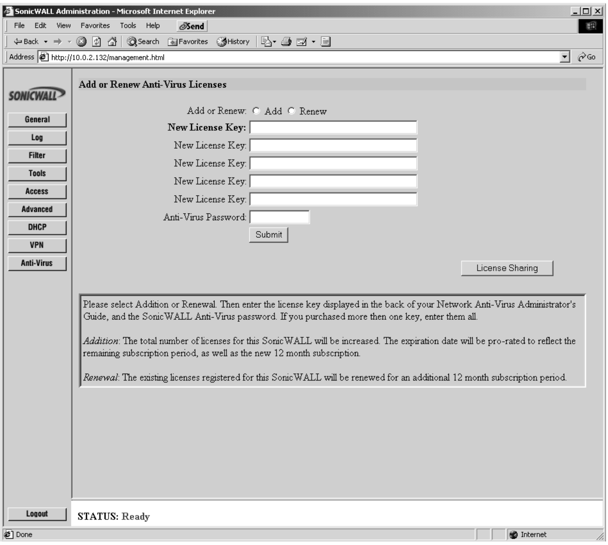
View Report

Change Anti-Virus Password

Add or renew Anti-Virus Licenses

STATUS: Ready

2. Click **Add / Upgrade Licenses**.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites History
Address http://10.0.2.132/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
Logout
Submit
License Sharing
Done
Internet

Add or Renew Anti-Virus Licenses

Add or Renew: ○ Add ○ Renew

New License Key:

New License Key:

New License Key:

New License Key:

New License Key:

Anti-Virus Password:

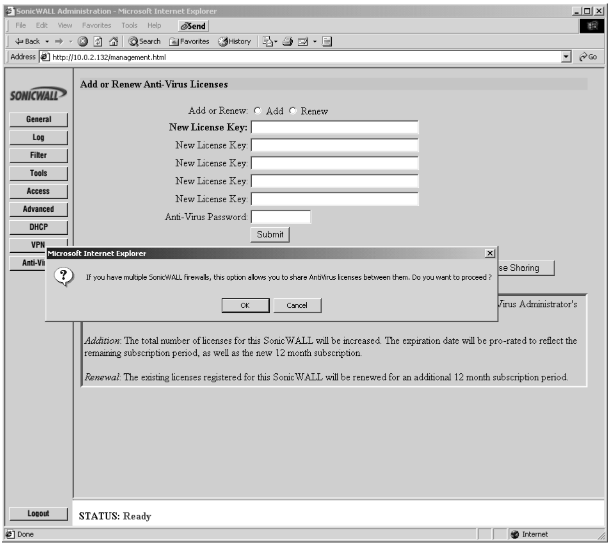
Please select Addition or Renewal. Then enter the license key displayed in the back of your Network Anti-Virus Administrator's Guide, and the SonicWALL Anti-Virus password. If you purchased more then one key, enter them all.

Addition: The total number of licenses for this SonicWALL will be increased. The expiration date will be pro-rated to reflect the remaining subscription period, as well as the new 12 month subscription.

Renewal: The existing licenses registered for this SonicWALL will be renewed for an additional 12 month subscription period.

STATUS: Ready

3. Click **License Sharing** to configure license sharing between SonicWALLs.


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites History
Address http://10.0.2.132/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Vi
Logout
Submit
se Sharing
Microsoft Internet Explorer
OK
Cancel
Done
Internet

Add or Renew Anti-Virus Licenses

Add or Renew: ○ Add ○ Renew

New License Key:

New License Key:

New License Key:

New License Key:

New License Key:

Anti-Virus Password:

If you have multiple SonicWALL firewalls, this option allows you to share AntiVirus licenses between them. Do you want to proceed ?

Virus Administrator's

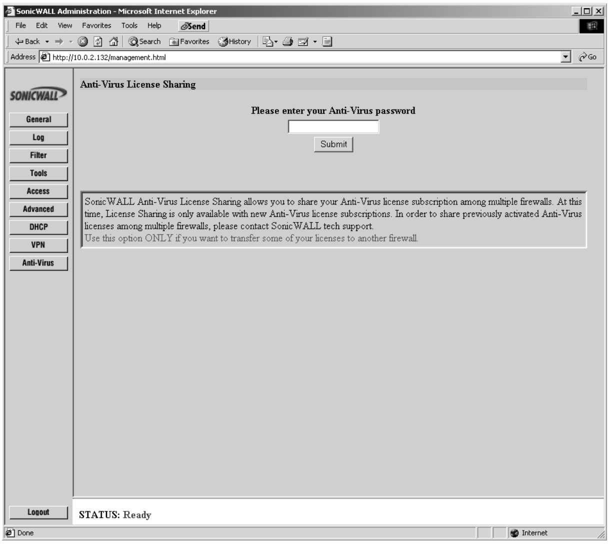
Addition: The total number of licenses for this SonicWALL will be increased. The expiration date will be pro-rated to reflect the remaining subscription period, as well as the new 12 month subscription.

Renewal: The existing licenses registered for this SonicWALL will be renewed for an additional 12 month subscription period.

STATUS: Ready

4. Click **OK** to configure the **License Sharing Group**.

5. Enter your Anti-Virus password to begin configuring the **License Sharing Group**, and click **Submit**.



SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites History
Address http://10.0.2.132/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
Logout
Done
Internet

Anti-Virus License Sharing

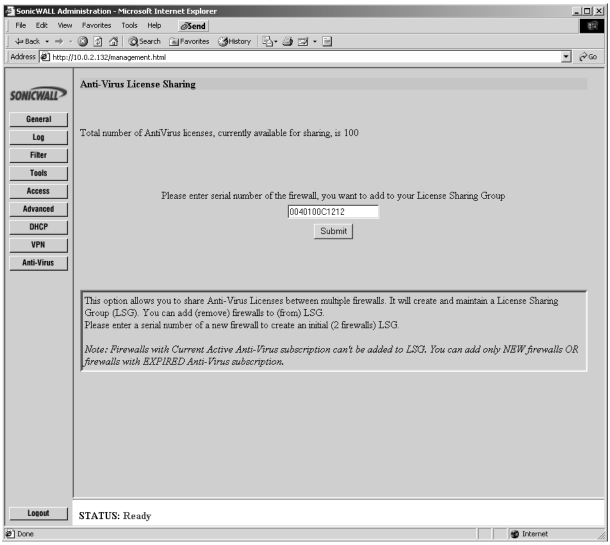
Please enter your Anti-Virus password

Submit

SonicWALL Anti-Virus License Sharing allows you to share your Anti-Virus license subscription among multiple firewalls. At this time, License Sharing is only available with new Anti-Virus license subscriptions. In order to share previously activated Anti-Virus licenses among multiple firewalls, please contact SonicWALL tech support.
Use this option ONLY if you want to transfer some of your licenses to another firewall.

STATUS: Ready

6. The **License Sharing Group** page appears and displays the number of available Anti-Virus licenses. Enter the serial number of the firewall to be added to your **License Sharing Group**, and click **Submit**.



SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites History
Address http://10.0.2.132/management.html
Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
Logout
Done
Internet

Anti-Virus License Sharing

Total number of AntiVirus licenses, currently available for sharing, is 100

Please enter serial number of the firewall, you want to add to your License Sharing Group

0040100C1212

Submit

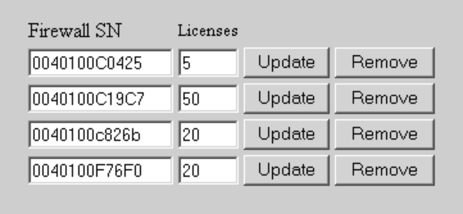
This option allows you to share Anti-Virus Licenses between multiple firewalls. It will create and maintain a License Sharing Group (LSG). You can add (remove) firewalls to (from) LSG.
Please enter a serial number of a new firewall to create an initial (2 firewalls) LSG.

Note: Firewalls with Current Active Anti-Virus subscription can't be added to LSG. You can add only NEW firewalls OR firewalls with EXPIRED Anti-Virus subscription.

STATUS: Ready

Note: *You can only add SonicWALL appliances to your group that do not have active Anti-Virus subscriptions. The SonicWALL appliance must also be registered at http://www.mysonicwall.com before it can be added to the group.*

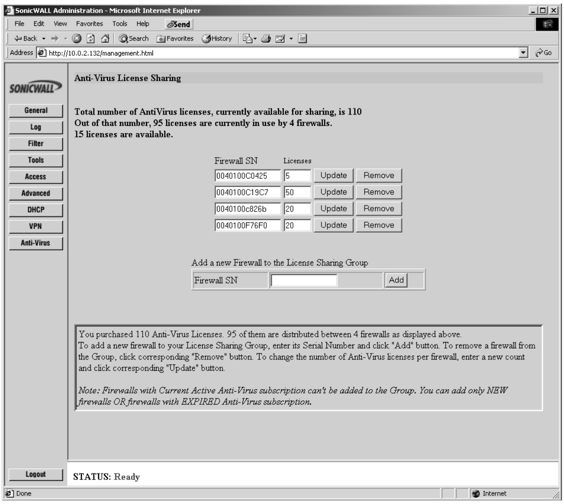
7. To distribute licenses between the SonicWALL appliance, enter the number of licenses for the first SonicWALL appliance into the **Licenses** field, and click **Update**. Repeat for each SonicWALL appliance.



Firewall SN	Licenses		
0040100C0425	5	Update	Remove
0040100C19C7	50	Update	Remove
0040100c826b	20	Update	Remove
0040100F76F0	20	Update	Remove

You can also remove a SonicWALL appliance or redistribute the number of licenses between the SonicWALL appliances. To remove a SonicWALL appliance, click **Remove** next to the SonicWALL serial number. To redistribute licenses, enter the new number of licenses into the **License** field and click **Update**. Repeat for each SonicWALL appliance.

The **License Availability** information changes as you change the license distribution or add more SonicWALL appliances. A typical **License Sharing Group** is displayed below:



Address: http://10.0.2.132/management.html

Anti-Virus License Sharing

Total number of AntiVirus licenses, currently available for sharing, is 110
Out of that number, 95 licenses are currently in use by 4 firewalls.
15 licenses are available.

Firewall SN	Licenses		
0040100C0425	5	Update	Remove
0040100C19C7	50	Update	Remove
0040100c826b	20	Update	Remove
0040100F76F0	20	Update	Remove

Add a new Firewall to the License Sharing Group

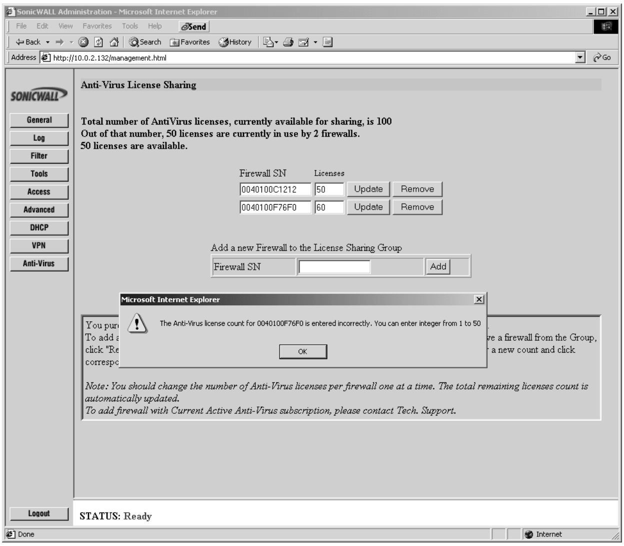
Firewall SN ____ Add

You purchased 110 Anti-Virus Licenses. 95 of them are distributed between 4 firewalls as displayed above.
To add a new firewall to your License Sharing Group, enter its Serial Number and click "Add" button. To remove a firewall from the Group, click corresponding "Remove" button. To change the number of Anti-Virus licenses per firewall, enter a new count and click corresponding "Update" button.

Note: Firewalls with Current Active Anti-Virus subscription can't be added to the Group. You can add only NEW firewalls OR firewalls with EXPIRED Anti-Virus subscription.

STATUS: Ready

If licenses are not available and you attempt to add more to the **License Sharing Group**, the following error message is displayed:


SonicWALL Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help Send
Back Search Favorites History
Address http://10.0.2.132/management.html Go
SONICWALL
General
Log
Filter
Tools
Access
Advanced
DHCP
VPN
Anti-Virus
Logout
Done
Internet

Anti-Virus License Sharing

Total number of AntiVirus licenses, currently available for sharing, is 100
Out of that number, 50 licenses are currently in use by 2 firewalls.
50 licenses are available.

Firewall SN	Licenses		
0040100C1212	50	Update	Remove
0040100F76F0	60	Update	Remove

Add a new Firewall to the License Sharing Group

Firewall SN [ ] Add

Microsoft Internet Explorer

The Anti-Virus license count for 0040100F76F0 is entered incorrectly. You can enter integer from 1 to 50

OK

You pur
To add a ve a firewall from the Group,
click "Re a new count and click
correspo

Note: You should change the number of Anti-Virus licenses per firewall one at a time. The total remaining licenses count is automatically updated.
To add firewall with Current Active Anti-Virus subscription, please contact Tech. Support.

STATUS: Ready

Anti-Virus Activation Key

SonicWALL, Inc.
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
Tel: 408-745-9600
Fax: 408-745-9300
E-mail: sales@sonicwall.com
Web: http://www.sonicwall.com

Part # 232-000068-03
Rev A 11/01